IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

CAPITOL RECORDS, INC., *et al.*,

Plaintiffs,

vs.

JAMMIE THOMAS,

Defendant.

Case No.: 06cv1497-MJD/RLE

PLAINTIFFS' RESPONSE TO MOTION TO SUPPRESS EVIDENCE

Plaintiffs submit this response in opposition to Defendant's Motion to Suppress Evidence (Doc. No. 263), and state as follows:

INTRODUCTION

Defendant's Motion to Suppress is premised on an entirely fictional set of facts and law. Factually, Defendant's Motion fundamentally misconstrues how information travels on the Internet, how KaZaA and the FastTrack network operate, and the actions taken by MediaSentry to record files and data sent to it. All of the information collected by MediaSentry was available to any user of the FastTrack network – millions of users at any given time. All MediaSentry did was record or document the information that was sent to it. The recording by a recipient of information sent to that recipient cannot be, and was not, a violation of the law and, as such, it should not be suppressed. Legally, it is hornbook law that the Fourth Amendment, and thus the exclusionary rule, does not apply in civil cases. And none of the statutes Defendant claims MediaSentry to have violated provide for exclusion of evidence. In short, MediaSentry did not violate any State or Federal law and there is no basis for excluding evidence gathered by MediaSentry.

Defendant's unsupported and unsubstantiated attacks on Plaintiffs (and their counsel) are simply unfounded. As numerous courts around the country have held, in considering similar claims made by other defendants in similar file-sharing cases, Plaintiffs actions in detecting and pursuing claims of copyright infringement were neither unethical nor illegal. Plaintiffs were simply protecting their rights and their intellectual property. As the Court explained in a similar file-sharing case, *Atlantic Recording Corp. v. Heslep*, 2007 U.S. Dist. LEXIS 35824, at *16 (N.D. Tex. 2007):

> The Court rejects [the defendant's] characterization of this lawsuit, and many others like it, as "predatory." Plaintiffs' attorneys brought this lawsuit not for the purposes of harassment or to extort [] as she contends, but, rather to protect their clients' copyrights from infringement and to help their clients deter future infringement. The evidence uncovered from MediaSentry's investigation shows that Plaintiffs' allegation of [] alleged copyright infringement have evidentiary support and will likely have more evidentiary support through further investigation and discovery. For now, our government has chosen to leave the enforcement of copyrights, for the most part, in the hands of the copyright holder. Plaintiffs face a formidable task in trying to police the internet in an effort to reduce or put a stop to the online piracy of their copyrights. Taking aggressive action, as Plaintiffs have, to defend their copyrights is certainly not sanctionable conduct under Rule 11. The right to come to court to protect one's property rights has been recognized in this country since its birth.

Id. at *16. It cannot be a violation of either the ethics rules or the law to log on to a peer-to-peer network, as any other user of the network could do, request copyrighted files being offered by users on the network, and then record the information sent. Indeed, Defendant has not – and cannot – cite a single authority that holds this conduct to be violative of laws or ethics. As such, Defendant's Motion to Suppress should be denied.

BACKGROUND

Peer-to-peer networks allow people to connect to each other to distribute files, including, in large measure, audio files containing popular copyrighted music. Unlike the World Wide Web (web sites) where data is stored on central web services and users connect to a central web server to download information from the web site, peer-to-peer networks allow users to connect to each other and transfer files directly from user to user. (Declaration of Doug Jacobson ("Jacobson Decl.") at ¶ 2, attached hereto as **Exhibit A**.)

When files are distributed from one user to another on the KaZaA peer-to-peer network, a set of identifiers tie the files back to the user distributing the files. These include (a) the IP address of the client distributing the files, (b) the name of the file, (c) file size, (d) the content hash, and (e) the port information. (*Id.* at ¶ 3.) At no time during the process of communicating or sharing files does one user gain entry into another user's computer. (*Id.* at ¶ 5.) Rather, the user requesting files simply communicates a request that the sharing computer send files, and the sharing computer sends the files. (*Id.*) Neither KaZaA, nor any other popular file-sharing program, permits one user to gain access into or in any way alter or manipulate the contents of another user's computer, or even to view any contents of another user's computer except those placed in a shared folder. (*Id.*)

In this case, MediaSentry did not need to take any kind of extraordinary steps in order to document the IP address of the computer from which it downloaded music files. (*Id.* at ¶ 6.) The IP address is transmitted as part of the normal process of connecting one computer to another over the Internet. (*Id.*) When identifying infringers on peer-to-peer networks, MediaSentry does only what any other user on the network can do. (Declaration of Chris Connelly ("Connelly Decl.") at ¶ 2, attached hereto as **Exhibit B**.) It uses the same network protocols used by every other user on the network to search for and download files. (*Id.*) Files transferred from the uploader's computer to MediaSentry are sent by the uploader in the form of data packets, which contain information identifying the source IP address, *i.e.*, the IP address for the computer from which the file is being transferred. (*Id.*) Using widely used packet capture technology, MediaSentry records the interaction between itself and a computer connected to the file sharing network at a specific IP address in order to show the file and data transfer from that computer. (*Id*.)[1] In other words, when downloading files from another user on a peer-to-peer network, the downloading process itself allows MediaSentry to identify the computer distributing the copyrighted material from a specific IP address. (*Id*.) MediaSentry captures this IP address information, along with other information about the file, including the specific date and time of file transfer. (*Id*.)

As numerous courts around the country have held, the information available on peer-to-peer networks is public information, readily accessible to anyone who wants it, and for which there is no reasonable expectation of privacy. *See In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003) (holding that when an ISP subscriber "opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."), *rev'd on other grounds*, 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 543 U.S. 924 (2004); *Elektra Entm't Group, Inc. v. Does 1-9*, 2004 WL 2095581, at *5 (S.D.N.Y. Sep. 8, 2004) (holding Defendant has "minimal 'expectation of privacy in downloading and distributing copyrighted songs without permission'"); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (activation of file-sharing mechanism shows no expectation of privacy); *Sony Music Entertainment Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004) ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission"); *Arista Records, L.L.C. v. Tschirhart*, Case

[1] Indeed, this packet capture technology is so ubiquotous that it is widely available for use on most major operating systems, including Windows. (Jacobson Decl. at ¶ 8.)

No. 05-CV-372-OLG, slip op. at 6 (W.D. Tex. May 24, 2006) (attached hereto as **Exhibit C**) ("[a] user of a P2P file-sharing network has little or no expectation of privacy in the files he or she offers to others for downloading").

ARGUMENT

Defendant seeks to suppress evidence gathered by MediaSentry arguing that MediaSentry violated (1) the Minnesota Private Detectives Act (the "MPDA"), the (2) the Pen Register and Trap and Trace Devices Act (the "Pen Register Act"), and (3) the Electronic Communications Privacy Act of 1986 (the "Wiretap Act"). As demonstrated below, not only is Defendant wrong on the facts, but she is wrong on the law as well.

I. MediaSentry Did Not Violate The MPDA.

A. The MPDA has no application to MediaSentry or its activities in this case.

Defendant's contention that MediaSentry violated the MPDA fails for several reasons. First, Defendant has not provided any authority to support the idea that MediaSentry is even subject to the MPDA. Nor could she. The MPDA does not apply to persons or companies operating outside of the State of Minnesota. *See* Minn. Stat. § 326.3381, subd. 5 (providing procedures for licensing out of state applicants who *"establish a Minnesota office.").* Minnesota's licensing scheme cannot apply to non-Minnesota entities conducting activities in other states, especially where such entities may be subject to other licensing requirements. *See Healy v. Beer Inst.*, 491 U.S. 324, 36 (1989) (a statute that seeks to control commerce occurring wholly outside the boundaries of a State "exceeds the inherent limits of the enacting State's authority and is invalid."). Here, MediaSentry does not operate in the State of Minnesota and conducted no investigation within the State of Minnesota that could possibly subject it to the State's licensure requirements. (Connelly Decl. ¶ 3.) MediaSentry has no employees in the State of Minnesota and does not conduct any activities in the State. (*Id.*) It does not pay taxes in

Minnesota and does not have an agent for service of process in the State. (*Id.*) Most significantly, MediaSentry conducted no activity whatsoever in the State of Minnesota relating to this case. (*Id.*) All of the information MediaSentry received was sent by Defendant from her computer to MediaSentry's computer in another state. (*Id.*)

Moreover, the MPDA regulates persons operating in quasi-police roles – applicants must spend a minimum of 6000 hours as an employee of a licensed private detective agency, or federal or state law enforcement agency in order to qualify. *See* Minn Stat. § 326.3382, subd. 2. As explained above, the type of work performed by MediaSentry, the gathering of public information that was placed on the Internet, does not come close to playing a quasi-police role and certainly does not implicate the MPDA. There was no private investigation here because the information that MediaSentry gathered is public information sent to MediaSentry by Defendant's computer, over a peer-to-peer network. (Connelly Decl. at ¶ 2; *see also* Jacobson Decl. at ¶ 6.)

Finally, Defendant has not cited any authority indicating that she has standing to assert claims under the MPDA. The MPDA contains no provision authorizing a private party to enforce the statute. Rather, the MPDA places exclusive enforcement authority in a Board of Private Detective and Protective Agent Services. *See* Minn. Stat. § 326.33 and 3311 (giving the Board authority "to enforce all laws and rules governing private detectives and protective agents" in Minnesota). Thus, Defendant lacks standing to enforce the MPDA. Because Defendant lacks standing to bring claims under the MPDA, the Court does not have jurisdiction to hear her argument. *See Faibisch v. Univ. of Minn.*, 304 F.3d 797, 801 (8th Cir. 2002) ("if a plaintiff lacks standing, the district court has no subject matter jurisdiction" over a claim).

B. The MPDA provides no basis for excluding any evidence in this case.

Not only has there been no violation of the MPDA, the MPDA provides no basis for excluding evidence. No provision of the MPDA supports the exclusionary rule as a remedy for alleged violations of the MPDA and no court has interpreted a violation of the MPDA to invoke the exclusionary rule. Indeed, the Federal District Court for the District of Maine, when interpreting a similar licensing statute, held that that failure of a witness to obtain a private investigator's license did not warrant excluding his testimony at trial. In *TNT Road Co. v. Sterling Truck Corp.*, 2004 U.S. Dist. LEXIS 13463, at * 6 (D. Me. July 19, 2004), the Court concluded that:

> Assuming that [the expert] was required by Maine law to have a license to conduct his investigation of the vehicle fire in this case, I am not persuaded that his failure to do so justifies the exclusion of his testimony. Nor do I think that his failure to obtain a license prevents the court from considering his expert qualifications or the reliability of his investigatory methods.

Id at * 6.

Furthermore, the single case cited by Defendant, *State v. Horner*, 617 N.W. 2d 789 (Minn. 2000), does not support applying the exclusionary rule under the MPDA or even in the civil context. In *Horner*, the Minnesota Supreme Court upheld a district court's suppression of evidence of the defendant's intoxication because the arresting officers were unpaid volunteers and lacked legal authority to perform tests for intoxication. *Id*. at 796. *Horner* also has no applicability to the facts in this case. The *Horner* court did not involve private investigators nor did it discuss the MPDA. Importantly, *Horner* is a criminal case, and the court never discussed whether suppression of evidence applies in a civil case such as this one.

For these reasons, the MPDA has no application here and provides no basis for excluding evidence.

II. MediaSentry Did Not Violate The Pen Register Act And, Under Established Eighth Circuit Precedent, The Exclusionary Rule Does Not Apply To The Pen Register Act As A Matter Of Law.

A. MediaSentry's actions do not violate the Pen Register Act.

Defendant alleges, with no support, that MediaSentry's recording of the IP address of the packets sent to it by Defendant somehow constitutes a violation of the Pen Register Act, 18 U.S.C. 3121 *et seq*., and that all MediaSentry-related evidence should be suppressed as a result. Defendant's argument is wrong and both fundamentally misconstrues the process through which MediaSentry obtained the evidence at issue and ignores binding Eighth Circuit precedent holding that the exclusionary rule has no application in the context of the Pen Register Act.

A "pen register" (and similarly a "trap and trace device") is a device or process used to record or decode dialing, routing or addressing information for transmissions of electronic communications. The Pen Register Act requires law enforcement, wishing to have a telephone or Internet Service Provider place a pen register or trap and trace device on a subscriber's phone or Internet line, to first apply to the Court and certify "that the information likely to be obtained is ***relevant*** to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2).

Here, the Pen Register Act is not implicated. Contrary to Defendant's assertion, the Pen Register Act does not apply because the "pen registers and trap and trace devices, by definition, do not record 'the contents of any communication.' 18 U.S.C. § 3127(3)-(4)." *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 450 (C.D. Cal. 2007); *see also* S.R. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3603 ("Pen registers do not record the contents of a communication" and "[t]rap and trace devices do not record the contents of communications"). In this case, the IP address was communicated to MediaSentry as part of the content of the

#1411218 v3 den

communication.[2] *See* Motion at 8 ("The TCP/IP packets that MediaSentry intercepted contain both recipient and sender IP addresses and the actual contents of the file being transferred over the Internet."). Specifically, the metadata that is transmitted along with every file sent through the Fasttrack network at issue in this case always includes the IP address. (Jacobson Decl. at ¶ 6.) The MediaSentry documents that Defendant seeks to suppress include content information, as well as IP addressing information. (Motion at 8.) Therefore, as the Court explained in *Bunnell*, the Pen Register Statute is "inapplicable" because the documents contain contents of communications. *Bunnell*, 245 F.R.D. at 450; *see also In re United States for an Order Authorizing the Use of a Pen Register & Trap,* 396 F. Supp. 2d 45, 50 (D. Mass. 2005) (interpreting "contents of communications" to include "application commands, search queries, requested file names, and file paths").

The Pen Register Act is intended to provide safeguards and procedure for law enforcement seeking to place pen registers or trap and trace devices on third-parties, either through a telephone company, ISP, or surreptitiously on a criminal suspect. *See* S.R. 99-541, at 1-5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555-3559 (intent of legislation based on "lack of clear standards [which] may expose law enforcement officers to liability and may endanger the admissibility of evidence"). It is not intended to prevent individuals who are receiving communications from recording information sent to them. If that were the case, standard computer operations that require recording of IP addresses so parties may communicate over the Internet would be prohibited and the Internet could not function. (*See* Jacobson Decl. at ¶ 4.)

---

[2] Indeed, it is impossible for the Internet to function without the transmittal of IP addresses between communicating computers. (Jacobson Decl. at ¶ 4.)

Furthermore, not only did the recording of IP addresses communicated to MediaSentry not constitute a trap and trace device, Defendant did not have a legitimate expectation of privacy in her IP address. As the Ninth Circuit explained in *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008):

> We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in [Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)]. First, e-mail and Internet users, like the telephone users in Smith, rely on third-party equipment in order to engage in communication. . . . Analogously, **e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit** because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," **e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers**.

See Smith v. Maryland, 442 U.S. 735 (1979) (holding that telephone users have no reasonable expectation of privacy in the telephone numbers they dial to connect a phone call); *United States v. Li*, 2008 U.S. Dist. LEXIS 22283, at *15 (S.D. Cal. Mar. 20, 2008) ("the court concludes that Defendant had no reasonable expectation of privacy in her IP log-in histories and IP addressing information.").

Additionally, the Pen Register Act does not prohibit recordings made with the consent of one of the parties. *See United States v. Millet*, 2005 U.S. Dist. LEXIS 26752, at *2 (N.D. Ill. Nov. 3, 2005) (rejecting a challenge to a government investigation, including the use of a pen register and/or trap and trace device, and holding that, "recordings made of conversations with the consent of one of the parties are permissible under federal law" and "pen registers and trap-and-trace devices . . do not disclose the contents of the conversations, ***nor do they make illegal the consensual recordings***."); *People v. Delacruz*, 156 Misc. 2d 284, 286 (N.Y. Sup. Ct. 1992) (in the context of an eavesdropping warrant, explaining that a third party "consented to having a trap and trace device placed on her phone."); *Ohio Domestic Violence Network v. Public Utils. Comm'n*, 70 Ohio St. 3d 311, 322 (Ohio 1994) (finding, in a single party consent state like Minnesota, that a subscriber "consents to the trap and trace, and thus that such services [as Caller ID] are not prohibited under the ECPA."); *S. Bell Tel. & Tel. Co. v. Hamm*, 306 S.C. 70, 71 n.1 (S.C. 1991) (finding, under South Carolina's Trap and Trace Law, that use of the device does not violate the law where "the consent of the user has been obtained.").

Here, the IP address was communicated as part of packets sent by Defendant from her computer to MediaSentry's computer. (Connelly Decl. at ¶ 2.) MediaSentry, a party to the communication, recorded the IP address and other information transmitted from Defendant's computer. (*Id.*) Therefore, to the extent such recording constitutes a trap and trace device, it was done with the consent of one of the parties to the communication, MediaSentry. As Minnesota is a single party consent state, the Pen Register Act does not apply. Minn. Stat. § 626A.02(2)(d) (it is legal for a person to record a wire, oral or electronic communications if that person is a party to the communication, or if one of the parties has consented to the recording).

B. Under established Eighth Circuit precedent, the exclusionary rule does not apply to the Pen Register Act.

In *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995), the Eighth Circuit held unequivocally that "the installation and use of a pen register is not a search within the meaning of the Fourth Amendment, and, therefore, its use does not violate the Constitution." The Court went on to hold that, "***the statutory scheme . . . does not mandate exclusion of evidence for violations of the statutory requirements***." *Id.* (emphasis added). Similarly, in *United States v. Olderbak*, 961 F.2d 756 (8th Cir. 1992), the Court stated, citing *Smith v. Maryland*, that "use of a pen register is not a 'search' under the fourth amendment and . . . . thus, regardless of whether the subpoena . . . was proper under state law . . . it is clear as a matter of federal law that the results of the pen register . . . were admissible." *See Smith v. Maryland*, 442 U.S. at 742-46 (holding use of a pen register does not implicate the Fourth Amendment because there is no reasonable expectation of privacy in phone numbers). As the Ninth Circuit explained in *United States v. Alba*, 2007 U.S. App. LEXIS 16147, at *18-19 (9th Cir. 2007):

> E-mail and Internet users have no expectation of privacy in the to-from addresses of their messages or the IP addresses of the websites they visit because they should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties. Communication by both Internet and telephone requires people to voluntarily turn over information to third parties.

Id. at *18-19. In this case, as explained above, MediaSentry simply recorded information sent to it from Defendant's computer over the Internet. As such, not only are MediaSentry's actions entirely appropriate, but Defendant had no reasonable expectation of privacy. The Eighth Circuit, as well as the United States Supreme Court, have rejected the suppression Defendant seeks.

III. MediaSentry Did Not Violate The Wiretap Act And The Act Does Not Provide For Exclusion Of Evidence.

A. MediaSentry's actions did not violate the Wiretap Act.

The Wiretap Act prohibits the *interception* of any wire, oral or electronic communication, without consent. 18 U.S.C. § 2511 *et seq.*[3] It does not prohibit the interception of a communication when "one of the parties . . . has given prior consent . . . ." 18 U.S.C. § 2511(2)(d).

---

[3] To the extent Defendant is arguing that MediaSentry illegally used a pen register or trap and trace device (Motion to Suppress at 8-9), such use is explicitly excluded from the purview of the Wiretap Act. *See Fregoso*, 60 F.3d at 1321.

Here, Defendant consented to the MediaSentry's download by placing the copyrighted sound recordings in a share folder accessible to the general public. *See In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d at 267 (When an ISP subscriber "opens his computer to permit others, through P2P file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."). In so doing, Defendant is not protected by the Wiretap Act. Additionally, regardless of whether Defendant consented, the communication at issue occurred between Defendant and MediaSentry, and there can be no dispute that MediaSentry consented to – indeed made – the recording at issue. *See Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364, at *41 (C.D. Cal. May 29, 2007) ("As defendants' website is the intended recipient of the Server Log Data, and defendants can lawfully intercept and consent to the disclosure thereof, this statutory provision, even if applicable would not provide a basis to withhold such data which is clearly within defendants' possession, custody and control.").

Defendant argues that the consent exception (18 U.S.C. §2511(2)(d)) does not apply because the communication was "intercepted for the purpose of committing any crime or tortious act." This is absurd. Plaintiffs gathered this information to protect their copyrights from rampant infringement on the Internet. *See, e.g., Heslep,* 2007 U.S. Dist. LEXIS 35824, at *16. Defendant offers no support for her contention that the communication was intercepted *for the purpose of* committing a crime or tort, and such an allegation is factually spurious. It makes no sense that MediaSentry would obtain information regarding Defendant's copyright infringement over a peer-to-peer network *for the purpose* of violating the MPDA or the Pen Register Act. And while Defendant and her counsel may disagree with Plaintiffs' decision to litigate cases like this one, there can be no question that gathering the evidence of Defendant's copyright infringement cannot be reasonably said to have been "for the purpose of committing" a crime or tort.[4] Therefore, Section 2511(2)(d)'s exception applies and MediaSentry's recording of the evidence of Defendant's copyright infringement does not fall within the confines of the Wiretap Act.

Further, the Wiretap Act states that it shall not be unlawful to "access an electronic communication made through a [computer] that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. §2511(2)(g)(i). This exception to protected communications specifically excludes Defendant from protection because she placed the sound recordings in a shared folder designed to be accessed by the general public. Defendant's argument that KaZaA is not open to the public is simply wrong. KaZaA and the FastTrack network at issue allow millions of users to trade files. Indeed, at the time Defendant's infringement was detected, 2,314,213 users like Defendant were online sharing files. (*See* Exhibit B to Complaint). Moreover, KaZaA is free and available to anyone who wants it and requires only basic registration information. (Jacobson Decl. at ¶ 7.) Obtaining and installing KaZaA can be done anonymously and easily by anyone with an Internet connection. (*Id*.) Moreover, contrary to Defendant's unsupported assertion, KaZaA does not require a password.

---

[4] While Defendant asserts, without support, that MediaSentry's actions constitute the tort of intrusion upon seclusion, such claims have been routinely rejected in similar file-sharing cases throughout the country. *See Tschirhart*, Case No. 05-CV-372-OLG, slip op. at 7 (holding that "there was no 'wrongful interference' because plaintiffs' investigators did not enter the private portion of her computer, but only accessed all publicly shared files.") (Ex. C); *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d at 267 (when an ISP subscriber "opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."); *Kennedy*, 81 F. Supp. 2d at 1110 (activation of file-sharing mechanism shows no expectation of privacy); *Does 1-9*, 2004 WL 2095581 at *5 (holding a defendant has "minimal 'expectation of privacy in downloading and distributing copyrighted songs without permission.'").

(*Id*.) There is no question that KaZaA is open and readily accessible to the general public.[5] The fact that the mechanical process requires downloading the software does not make it non-public because the software is available to anyone on the Internet.

Moreover, the Wiretap Act is not implicated in this case because, as to electronic communications, it only prohibits ***interception*** during transmission (not while in electronic storage, i.e., RAM), and the disclosure of electronic communications intercepted during transmission. *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 878-79 (9th Cir. 2002). Here, MediaSentry did not *intercept* the electronic communication during transmission but merely recorded and retained the electronic communication after it was sent directly to it.

B. The Wiretap Act does not provide for exclusion of evidence.

The exclusionary provision of 18 U.S.C. § 2515 applies to "wire and oral communication[s]" but not to "electronic communications" as defined in the Act. *See United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003) ("By its terms, 18 U.S.C.S. § 2515 applies only to wire communications, and not to electronic communications.") A "wire or oral communication" under the Wiretap Act typically involves an actual aural communication between persons. *See Lanier v. Bryant*, 332 F.3d 999, 1002 (6th Cir. 2003) (involving intercepted telephone conversations). Since the communication at issue here was electronic, the statute itself rejects exclusion, even in criminal cases. Additionally, the exclusionary provision of 18 U.S.C. § 2515 was not meant to apply in a civil proceeding. *See Philadelphia Resistance*

---

[5] Defendant's argument that the KaZaA terms of use show that KaZaA was not generally accessible to the public is both incorrect and a red herring. It would be ironic indeed if the terms of use of KaZaA could somehow immunize copyright infringers and prevent copyright holders from protecting their copyrights. Defendant has no right to enforce the KaZaA terms of use. To the extent the KaZaA terms of use suggest that a copyright holder cannot enforce its rights, they are ultra vires and without effect. Defendant cannot hide behind the KaZaA terms of use to shield her illegal activity.

v. Mitchell, 58 F.R.D. 139, 147 (E.D. Pa. 1972) ("Congress only intended to limit discovery in the context of criminal and not civil proceedings.")

IV. There Is No Basis For Suppression In This Case.

This is a civil matter that does not involve any government action that would invoke the Fourth Amendment, and thus the exclusionary rule should not apply. As the Supreme Court explained in *United States v. Janis*, 428 U.S. 433, 447 (1976), "In the complex and turbulent history of the [exclusionary] rule, the Court never has applied it to exclude evidence from a civil proceeding, federal or state." *See Thompson v. Carthage Sch. Dist.*, 87 F.3d 979, 981-982 (8th Cir. 1996); *United States v. Tauil-Hernandez*, 88 F.3d 576, 581 (8th Cir. 1996) ("The Supreme Court has declined various invitations to extend the Fourth Amendment exclusionary rule beyond the criminal trial."). *See also Vander Linden v. United States*, 502 F. Supp. 693, 696 (S.D. Iowa 1980) ("On a number of occasions the United States Supreme Court has stated that the purpose of the exclusionary rule is to safeguard Fourth Amendment rights by deterring future and unlawful police conduct."); *Mejia v. City of New York*, 119 F. Supp. 2d 232, 254 (S.D.N.Y. 2000) ("the Fourth Amendment's exclusionary rule does not apply in civil actions other than civil forfeiture proceedings.") (*citing Pennsylvania Bd. of Probation & Parole v. Scott*, 524 U.S. 357, 363 (1998)).

Moreover, not one of the federal or state laws which Defendant references in her Motion to Suppress provides for the exclusion of evidence as a remedy for violating the statutes at issue. And, in fact, the case law, and in the case of the Wiretap Act, the statute itself, specifically reject suppression. *See, supra,* Argument, Sections I, B; II, B; and III, B.

V. Suppression For Violation Of Ethics Rules Is Unprecedented And Would Be Inappropriate Here.

Recognizing that the federal and state authorities relied upon do not support the exclusion of evidence in this case, Defendant resorts to arguing for exclusion based on the rules of ethics. Of course, Defendant has not and could not cite a single authority to support her claim that Plaintiffs or their counsel have in any way violated any rule of ethics. This argument is merely an unfortunate, and unprofessional attack made in a desperate attempt to suppress evidence that Defendant and her counsel know is ruinous to her defense.

Leaving aside Defendant's unprofessional attack on the integrity of Plaintiffs and their counsel, which merits no further response, the cases that Defendant relies on, *Aiken v. Business and Indus. Health Group*, 885 F. Supp. 1474 (D. Kan. 1995), *State v. Ford*, 539 N.W. 2d 214 (Minn. 1995), and *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. App. 2005), do not support her arguments for suppression.

In *Aiken*, the court held that Rule 4.2 of the ABA Model Rules of Professional Conduct does not bar opposing counsel from ex parte contact with former employees of an organizational party represented by counsel. *Aiken*, 885 F. Supp. at 1475. The court discussed suppression in the context of warning counsel not to induce or listen to privileged communications from former employees and advised that information obtained in violation of counsel's ethical responsibilities could be "subject to suppression." *Id*. at 1480. The court suppressed no evidence and did not discuss the calculus for when or what evidence might be suppressed for a violation of ethical rules.

In *Ford*, the Minnesota Supreme Court affirmed a trial court's decision not to exclude evidence in a criminal case. The defendant in *Ford* made two statements to homicide detectives without his attorney present, though the detectives informed the defendant on both occasions of his constitutional rights. *Ford*, 539 N.W. 2d at 223. Because the trial court found the detectives' actions were not egregious, the Supreme Court affirmed the admission of the statements. *Id*. at 225. In discussing the defendant's arguments for exclusion of evidence, the *Ford* court made clear the court's precedent "*did not create an automatic exclusionary rule for a violation of Rule 4.2*." *Id*. (emphasis provided).

Finally, the *O'Brien* case cuts directly against Defendant's argument. In *O'Brien*, the trial court found that electronic communications were illegally obtained in violation of a state statute. *O'Brien*, 899 So. 2d at 1134. In determining the remedy for this violation, the Court "conclude[d] that the intercepted electronic communications in the instant case are not excludable under the Act" because the statute did not call for exclusion of intercepted electronic communications. *Id.* at 1137 (excluding evidence on grounds other than violation of the statute). Furthermore, the facts of *O'Brien* involve a wife copying and storing electronic communications between her husband and another woman. *Id*. at 1134. The wife's actions in *O'Brien* were illegal because Florida is a *two-party consent* state in regards to recording communications. Fla. Stat. § 934.03(2)(d) ("It is lawful . . . for a person to intercept a wire, oral, or electronic communication when all of the parties to the communication have given prior consent to such interception."). Minnesota, in contrast, is a *single-party consent* state. Minn. Stat. § 626A.02, subd. (2)(d) ("It is not unlawful . . . for a person . . . to intercept a wire, electronic, or oral communication, where such person is a party to the communication"). As a result, any argument that *O'Brien* should apply in this case lacks merit because the state laws on recording communications are entirely distinct from one another.

In this case, Defendant, apparently acknowledging that the statutes at issue do not provide for exclusion, attempts to bootstrap the alleged statutory violations with unsupported claims that Plaintiffs' counsel somehow violated their ethical obligations, and therefore, there is some sort of moral imperative of exclusion. However, where the statutes and case law specifically reject exclusion, the ethics rules cannot revive it. Defendant has not cited a single case where a court, citing to any state, federal or model ethics rules, excluded evidence allegedly obtained in violation of a state private detectives licensing statute or federal or state wiretapping or eavesdropping laws.

CONCLUSION

If simply recording an IP address and metadata sent to someone over the Internet was illegal, copyright holders would be unable to protect their content on the Internet. Defendant used the KaZaA peer-to-peer file sharing program to download and distribute Plaintiffs' copyrighted sound recordings. The recordings in Defendant's shared folder could have been downloaded by any one of the millions of users of the FastTrack network. MediaSentry was one of those users and, and instead of simply downloading the copyrighted sound recordings from Defendant, it downloaded the files and recorded the metadata and transmission data associated with those files as they were sent from Defendant to MediaSentry.

WHEREFORE, Plaintiffs ask that the Court deny Defendant's motion to suppress evidence.

Respectfully submitted this 4th day of June 2009.

/s/ Timothy M. Reynolds
Timothy M. Reynolds (pro hac vice)
David A. Tonini (pro hac vice)
Andrew B. Mohraz (pro hac vice)
HOLME ROBERTS & OWEN LLP
1700 Lincoln, Suite 4100
Denver, Colorado 80203
Telephone: (303) 861-7000
Facsimile: (303) 866-0200

Felicia J. Boyd (No. 186168)
Leita Walker (No. 387095)
FAEGRE & BENSON LLP
2200 Wells Fargo Center
90 South Seventh Street
Minneapolis, Minnesota 55402-3901
Telephone: (612) 766-7000
Facsimile: (612) 766-1600

ATTORNEYS FOR PLAINTIFFS